

## Cisco Configuration Engine 3.5

### **Q. What is Cisco® Configuration Engine?**

**A.** Cisco Configuration Engine is a highly scalable network management software application designed to facilitate rapid configuration and image distribution to thousands of devices simultaneously. Using Cisco IOS® Software agents, Cisco Configuration Engine provides zero-touch deployment (ZTD) and near-ZTD by eliminating the traditional device staging process. Using Cisco Configuration Engine for both rapid deployment and ongoing configuration and image updates can drastically reduce operating expenses (OpEx), especially for networks with a large number of remote devices.

### **Q. What is new in Cisco Configuration Engine 3.5?**

**A.** Cisco Configuration Engine 3.5 provides the following new features and supports:

- Operating-system support:
  - Solaris 10
  - Red Hat Linux 4.0 and 5.0
- VMware support
- **Automated port assignment:** This enhancement simplifies the bootstrap configuration process by allowing the Cisco Configuration Engine to dynamically assign the port number for device-to- Cisco Configuration Engine connections. With this feature, the bootstrap configuration is the same across all remote devices, regardless of the number of devices being managed.
- **External user authentication with Microsoft Active Directory:** This feature provides the flexibility of user authentication using an external Active Directory in addition to server-based local authentication.
- **Dual-zone support:** This feature allows the separation of different network zones between device access and the Cisco Configuration Engine application, providing more flexibility for security zoning requirements.
- **Support of Cisco Unique Device Identifier (UDI) as device identification:** This feature allows use of the Cisco product UDI as the unique device identification.
- **Secure FTP support:** With this feature, you can securely import and export configuration templates using Secure FTP.

### **Q. Cisco has previously offered a product called the Cisco Networking Services IE 2100 Intelligence Engine, which also uses Cisco IOS agent technology. What is the difference between the Cisco Networking Services IE 2100 Intelligence Engine and the Cisco Configuration Engine?**

**A.** The Cisco Networking Services IE 2100 Intelligence Engine is an older appliance that is in the end-of-life stage. Although both the Cisco IE 2100 and the Cisco Configuration Engine use the CNS technology, newer CNS agent features are supported only by the Cisco Configuration Engine. The Cisco Configuration Engine also provides higher scaling than the Cisco IE 2100.

**Q. What are zero-touch deployment and near-zero touch deployment?**

- A.** Zero-touch deployment (ZTD) refers to the deployment process such that no user interaction with the device is required other than connecting the necessary cables and powering up to bring up the remote device to its desired configuration. Near-ZTD refers to the fact that in the deployment process the only required user interaction with the remote device is connecting the necessary cables and powering up to bring up the device to its desired configuration. In both ZTD and near-ZTD, device staging is not required; furthermore, technical expertise—especially knowledge of the command-line interface (CLI) configuration—is not required in the remote location.

**Q. How is the Cisco Configuration Engine different from other deployment tools?**

- A.** Traditional management tools typically use Telnet or the Secure Shell (SSH) Protocol to log in to the devices and apply configurations. This process emulates and potentially automates a network engineer's manual process. The deployment process using the traditional approach requires coordination between the deployment personnel and the network operations center (NOC) so that a NOC engineer knows when to start logging in to the devices.

In contrast, the Cisco Configuration Engine uses deployment agents to accomplish most of the work. The deployment agents are called the CNS agents, which act as the deployment personnel by asynchronously initiating connection back to the Cisco Configuration Engine located in the NOC. By preparing the Cisco Configuration Engine appropriately to accept and process the connection request, the Cisco Configuration Engine positively identifies the device, generates the full configuration, and automates the CNS agents to apply the configuration to bring up the device. This distributed-agent approach eliminates the need for coordination between the deployment personnel and the NOC, and provides a highly scalable deployment solution.

**Q. Do we need to install the CNS agents onto the devices?**

- A.** No. The CNS agents come with Cisco IOS Software. Please confirm with your account representative to ensure the necessary CNS agents are supported by the platform and by the Cisco IOS Software image version. For information about what Cisco devices are supported by the Cisco Configuration Engine, please refer to the Cisco Configuration Engine data sheet.

**Q. My network has some devices that do not provide CNS agent support; can I still use the Cisco Configuration Engine to manage them?**

- A.** Yes, but with some limitations. The Cisco Configuration Engine provides a module called the Intelligent Modular Gateway (IMGW) Device Module Development toolkit to allow customized device access plug-in. The toolkit defines the southbound interface of the IMGW and provides a registration utility to allow you to register plug-in device modules into IMGW. The plug-in, typically a set of scripts, allows IMGW to access the device. These devices are called non-agent devices in Cisco Configuration Engine. Because there is no agent to initiate connections, the Cisco Configuration Engine does not support ZTD for non-agent devices; further, because there is no agent to provide distributive configuration and image update tasks, the total scaling and performance of the Cisco Configuration Engine are less than those of CNS agent-enabled devices.

For more information about developing a plug-in, please refer to the Cisco Configuration Engine User Guide located in the software CD.

**Q. How does the device know how to initiate connection back to the Cisco Configuration Engine?**

- A.** The device needs to have a bootstrap configuration, including three important steps:
- Establish IP connectivity if it is not available yet. Optionally, you can specify more security measures such as encryption, tunneling, and authentication.
  - Indicate where to “call home”—the Cisco Configuration Engine IP address.
  - Indicate the identification method for the CNS agents—the way that the agents should identify themselves to the Cisco Configuration Engine.

It is important to note that the bootstrap configuration can be the same across all your remote devices. This feature makes staging, if needed, much easier because you do not have to match the device with the right configuration.

**Q. What are the different identification methods for the CNS agents?**

**A.** Any unique string will work, as long as there is no overlap within the Cisco Configuration Engine. It is recommended you use identification methods that come with the devices, including hardware serial number and the Cisco product UDI. In some solutions such as Cisco Virtual Office, you can even use the end-user's username as the device identifier. It is important to note that the device identifier must be registered to the Cisco Configuration Engine so that it knows this device will be connecting.

**Q. Is there more than one way to put the bootstrap configuration into the devices?**

**A.** There are several ways of loading the bootstrap configuration into the devices:

- **AutoInstall:** AutoInstall is a Cisco IOS Software feature. A device having no configuration goes through a series of initial tasks, including sending out a Dynamic Host Configuration Protocol (DHCP) discover request. If the request reaches a DHCP server, the server can reply with an offer. Through DHCP option 150, the DHCP server can return a Trivial File Transfer Protocol (TFTP) address. The Cisco IOS Software device then requests the bootstrap configuration from the TFTP address. Because the bootstrap configuration is the same across all devices, for the configuration engine this option provides a true ZTD solution. The critical limitation is that the initial DHCP discover request must be able to reach the intended DHCP server—in many cases over a WAN.
- **Cisco IOS Software Secure Device Provisioning (SDP) in the Cisco Virtual Office solution:** The Cisco Virtual Office solution uses the Cisco IOS Software SDP feature along with Cisco Secure Access Control Server (ACS) to provide secure authentication of the device, and uses SDP to deliver the bootstrap configuration to the device. Please visit [www.cisco.com/go/cvo](http://www.cisco.com/go/cvo) for more details. The critical limitation is that this approach assumes that IP connectivity is already in place.
- **Cisco Configuration Express:** Cisco Configuration Express is an ordering option of selected hardware platforms. Using Cisco Configuration Express, you can specify the bootstrap configuration to be loaded into the devices before they are shipped. Because the bootstrap configuration is already loaded into the devices, the devices already have enough information to initiate connection to the Cisco Configuration Engine, thereby achieving ZTD. Please contact your Cisco account representative for more details and the models that are supported.
- **Aladdin eToken:** You can use the secure eToken USB key on the USB port for selected integrated services routers (ISRs). You can configure the ISRs to get bootstrap configuration from the secure eToken. For more information about Aladdin eToken, please contact your local Cisco account representative.
- **Staging:** You can also stage the devices using your existing staging service to put the bootstrap configuration onto the devices. Because the bootstrap configuration is the same for all devices, the staging process can be significantly simpler.

**Q. I want to use the AutoInstall option. Do I need to order the device with a certain option?**

**A.** Yes. In order for AutoInstall to be activated, the device must not have any configuration. For Cisco ISR and Cisco Integrated Services Routers Generation 2 (ISR G2) routers, please use the ISR-CCP-EXP-NOCONF or ISR-CCP-CD-NOCONF option when ordering Cisco 1900, 2900, and 3900 routers, and the CCP-EXPRESS-NOCF or CCP-CD-NOCF option when ordering Cisco 800, 1800, 2800, and 3800 routers

**Q. Who can benefit by using the Cisco Configuration Engine?**

**A.** Any network operation with a large number of remote devices can benefit from this application. Many service providers and enterprise customers have demonstrated huge reductions in OpEx in deployment and ongoing management using the Cisco Configuration Engine.

**Q. Can I integrate my operations-support-system (OSS) application with Cisco Configuration Engine?**

**A.** Yes, you can integrate Cisco Configuration Engine with just about any OSS. With the Web Services application programming interfaces (APIs), you have programmatic access to every feature inside Cisco Configuration Engine. With the Software Development Kit (SDK) you can easily obtain any data from Cisco Configuration Engine and direct it as though it is part of the OSS itself. You can purchase the optional SDK to integrate with the Cisco Configuration Engine. Please refer to the ordering guide for additional information.

**Q. What kind of hardware is required to support Cisco Configuration Engine?**

**A.** Cisco Configuration Engine will run on a wide variety of Sun- and PC-based hardware. For specific details, please refer to the data sheet.

**Q. Does the Cisco Configuration Engine provide an appliance option?**

**A.** No. The Cisco Configuration Engine is a software product.

**Q. What operating systems and versions does Cisco Configuration Engine support?**

**A.** The Cisco Configuration Engine Version 3.5 supports Solaris, Red Hat Linux, and VMware. For specific details, please refer to the data sheet.

**Q. How many devices can Cisco Configuration Engine support?**

**A.** Cisco Configuration Engine 3.5 supports up to 30,000 devices on a single Solaris server and up to 20,000 devices on a single Linux server. You can achieve higher scaling by using a load balancer such as the Cisco Content Switching Module as a front end to multiple Cisco Configuration Engines.

For recommended server configurations and respective scaling specifications, please refer to the ordering guide for additional information.

**Q. Is the Cisco Configuration Engine product highly available?**

**A.** You can achieve fault tolerance by placing multiple configuration engines behind a Cisco Load Balancer. Please ask your Cisco account representative for the Cisco validated design for this solution.

**Q. Do I need Cisco Configuration Engine if I have another management product from Cisco?**

**A.** Maybe. Depending on your needs and the other products installed, you may need Cisco Configuration Engine to meet your speed and scalability requirements. Ask your Cisco account representative for more information with deference to your unique environment.

**Q. Is there any Cisco network management application that integrates with the Cisco Configuration Engine?**

**A.** Yes. Cisco Security Manager and Cisco IP Solution Center both integrate with the Cisco Configuration Engine, taking advantage of the highly scaling configuration and image distribution capability of Cisco Configuration Engine.

**Q. Is there any Cisco Validated Design solution that uses the Cisco Configuration Engine?**

**A.** Yes. Cisco provides many Cisco Validated Designs to help customers easily implement specific networks.

The Cisco Virtual Office solution is an integrated solution to provide ZTD for remote teleworkers and small offices to support data, security, voice, and wireless services. For more information, please refer to <http://www.cisco.com/go/cvo>.

Other Cisco Validated Designs also use the Cisco Configuration Engine. Please contact your account representative for more details.

**Q. Can I evaluate Cisco Configuration Engine?**

**A.** Yes, you can. Please contact your account representative to get started.

**Q. What do I need to order to use Cisco Configuration Engine?**

**A.** Cisco Configuration Engine has two parts of licensing: server licenses and device Right-to-Use (RTU) licenses. To install the Cisco Configuration Engine, you need a server license per server instance; to use the Cisco Configuration Engine to manage devices, you need the device RTU license pack. Please ensure the total number of device licenses in the RTU license packs is equal or greater than the number of devices you plan to manage.

For more details about ordering, please contact your Cisco account representative.

**Q. I need to use Cisco Configuration Engine only for deployment. Can I reuse the device licenses for other devices after I have finished with the deployment?**

**A.** No. The device RTU licenses are associated with the devices that are or have been managed by the Cisco Configuration Engine.

**Q. Can I integrate my provisioning system with the Cisco Configuration Engine?**

**A.** Yes. The Cisco Configuration Engine provides a SDK to allow you to integrate your application with the Cisco Configuration Engine.

**Q. Can I use an external Lightweight Directory Access Protocol (LDAP) server with Cisco Configuration Engine?**

**A.** You can configure Cisco Configuration Engine to use either an internal or external LDAP server. You can select the type of LDAP server to be implemented through the configuration engine setup utility. You do not have to configure LDAP itself when using internal LDAP. If you decide to use an external LDAP server, you need to extend the vendor's LDAP schema to be able to support Cisco Configuration Engine-specific object classes that are needed to represent the server and devices. For external LDAP configuration, you must follow the LDAP vendor's installation and configuration procedures.

**Q. How do I stop or start the internal LDAP server?**

**A.** In order to gracefully shut down the internal LDAP server on the Cisco Configuration Engine server, use the following command: **`/etc/init.d/NetAppOpenLDAP stop to stop OpenLDAP server`**. The **`NetAppOpenLDAP stop`** command also performs data recovery to ensure data integrity.

To start the internal LDAP server, execute the following command: **`/etc/init.d/NetAppOpenLDAP start`**.

When the LDAP server is not shut down gracefully by **`NetAppOpenLDAP`** because of system crash, power outage, or manual shut down, data corruption may occur and the LDAP server will not respond. To fix the problem, stop the OpenLDAP server and run the following command to recover data:

**`/etc/init.d/NetAppOpenLDAP stop`**

**`${CISCO_CE_INSTALL_ROOT}/bdb/bin/db_recover -h`**

**`${CISCO_CE_INSTALL_ROOT}/openldap/var/openldap-data`**

**Q. How do I stop or start the Cisco Configuration Engine processes?**

**A.** The following list covers the Cisco Configuration Engine processes that are invoked during the application initialization:

- Configuration-engine monitor server: **`/etc/rc.d/init.d/MonitorCE stop / start`**
- Event gateway: **`/etc/rc.d/init.d/EvtGateway stop /start`**
- Event gateway with cryptography: **`/etc/rc.d/init.d/EvtGatewayCrypto stop / start`**
- IMGW: **`/etc/rc.d/init.d/lmgw stop / start`**

- HTTPd: **/etc/rc.d/init.d/httpd stop /start**
- OpenLDAP server: **/etc/rc.d/init.d/NetAppOpenLDAP stop /start**
- Tibco: **/etc/rc.d/init.d/tibco stop / start**
- Lock monitor server: **/etc/rc.d/init.d/LockMonitor stop / start**

**Q. Where are Cisco Configuration Engine log files located?**

**A.** Cisco Configuration Engine offers log files for the main configuration-engine components. The most important ones are located in: /var/log/CNSCE. The following list offers the log file names and their related components:

- appliance-setup.log: Status of setup, start, or shutdown of the Cisco Configuration Engine
- websvc/websvc.log: Web service general log
- cfgsrv/cfgsrv.log: Config service log
- imgsrv/imgsrv.log: Image service log
- cfgsrv/exec-srv.log: Exec service log
- ce\_monitor/ce\_monitor.log: Configuration-engine health status
- tomcat: Tomcat server logs
- evtgateway: Event-gateway log (to see this log, you have to turn it on during setup)

**Q. What is a TibGate?**

**A.** Devices connect to the Cisco Configuration Engine through TCP/Secure Sockets Layer (SSL) connection; this connection is made to the event gateway or TibGate. Each TibGate port within Cisco Configuration Engine serves 500 devices.

TibGates are associated with port numbers. The Cisco Configuration Engine uses odd port numbers starting at 11011 for nonsecured device communication, and even port numbers starting at 11012 for secured device communication. You can check the status of a specific TibGate with the following command:

**/etc/init.d/EvtGateway status <port number>.**

You can manually stop or start a specific TibGate with the following command: **/etc/init.d/EvtGateway {stop / start} <port number>.**

For cryptography devices use: **/etc/init.d/EvtGatewayCrypto {status | {start / stop} [port number]}.**

The configuration-engine installation process performs a series of hardware checks to determine the number of CPUs, memory, and swap space in the system. Based on these parameters it determines the number of supported event gateways for the particular server.

**Q. Why does a provisioned device still show up "RED" on the Cisco Configuration Engine web interface?**

**A.** There are multiple reasons.

- To start, make sure that the device being provisioned has IP connectivity with the configuration-engine server and conversely, perform a **ping** command.
- Second, make sure that the "Device ID" assigned on the bootstrap configuration file matches the one provisioned on the web interface.
- Third, if device authentication is enabled, check the password in the device. Also make sure that the device password is synchronized with the Cisco Configuration Engine.

**Q. I am having trouble managing a device with Cisco Configuration Engine. How do I troubleshoot this problem?**

**A.** It is important when you have connectivity problems with the provisioned device that you turn debug on. You need to use Telnet to your device and execute the following commands:

- **Device> config t**

- **Device> enable**
- **Device# debug cns all**
- **Device# ter mon**

The debug cns all command will give you the most output when the device and the configuration-engine server are trying to establish connectivity. You can also use the **debug cns ?** command to obtain list of the available Cisco Networking Services commands.

**Q. Where can I find out more about Cisco Configuration Engine?**

**A.** For more information about Cisco Configuration Engine, please visit <http://www.cisco.com/en/US/products/sw/netmgtsw/ps4617/index.html>.



Americas Headquarters  
Cisco Systems, Inc.  
San Jose, CA

Asia Pacific Headquarters  
Cisco Systems (USA) Pte. Ltd.  
Singapore

Europe Headquarters  
Cisco Systems International BV  
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1002R)